REMARKS

This response is a full and complete response to the Final Office Action dated November 27, 2006. In the present Office Action, claims 1-31 are pending in the application, claims 1-3, 10-12, 20-23, and 31 stand rejected, claims 4-9, 13-19 and 24-30 are objected to, and no claims have been allowed.

In view of both the amendments previously presented and the following remarks, it is submitted that the claims pending in the application are nonobvious. It is believed that this application is in condition for allowance. By this response, entry of the amendment and reconsideration of the present application are respectfully requested.

ALLOWABLE SUBJECT MATTER

Assignee's representative thanks the Examiner for continuing to identify claims 4-9, 13-19, and 24-30 as being allowable if rewritten in independent form including all the limitations of the base claim and any intervening claim. In light of the remarks below and the amendments above, it has been decided to continue deferring without prejudice rewriting the claims in independent form to a later time in the prosecution, if at all.

CITED ART

U.S. Patent 6,052,466 to Wright ("Wright"), U.S. Patent 6,159,633 to Nakamura ("Nakamura"), and U.S. Patent 6,192,129 to Coppersmith et al. ("Coppersmith") are all cited and applied in the present Office Action.

CLAIMS REJECTIONS UNDER 35 USC § 103

Claims 1-3, 10-12, 20-23, and 31

Claims 1-3, 10-12, 20-23, and 31 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Wright and further in view of Nakamura and Coppersmith. This rejection is respectfully traversed.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art references when combined must teach or suggest all the claim limitations. (See MPEP § 2142.). Motivations to combine or modify references must come from the references themselves or be within the body of knowledge in the art. (See MPEP § 2143.01.)

Independent claim 1 calls for:

> *In an apparatus, a method of operation comprising:*
> *generating in real time a first deciphering round key based on a deciphering key;*
> *incrementally deciphering a ciphered text for a first round using the real time generated first deciphering round key to generate a partially deciphered text;*
> *generating in real time a second deciphering round key based, at least in part, on said generated first deciphering round key while said incremental deciphering for said first round is being performed; and*
> *incrementally deciphering the partially deciphered text for a second round using the real time generated second deciphering round key.*

Wright appears to teach encryption of data packets using a sequence of private keys generated from a public key exchange wherein each data packet is enciphered and then deciphered using a single stream cipher produced by a particular private key called a secondary key. When the stream cipher is applied once to an enciphered data packet, the data packet is completely deciphered into clear text from this single application of the key. When the next enciphered packet arrives, a new stream cipher is selected. The new stream cipher is then applied to the newly arrived enciphered packet to decipher the packet completely into clear text by this single application of the new stream cipher. In Wright, one application of the stream cipher changes the enciphered packet into clear text once and for all. There are no multiple rounds or multiple ciphers needed to decrypt the packet in Wright. A single cipher decrypts its associated packet completely by one application of the cipher. There is no teaching or remote suggestion in Wright concerning incremental deciphering.

Incremental deciphering defined in claim 1 initially requires a first round of deciphering using the first deciphering round key to generate the partially deciphered text. *See third paragraph of claim 1 above beginning at "incrementally".* Then the incremental deciphering is performed on the partially deciphered text using a second deciphering round key. *See fifth paragraph of claim 1 above beginning at "incrementally".* This is clearly different from Wright in that multiple rounds of deciphering are performed on the ciphered text and the incremental (partial) decipherings thereof in order to begin to complete the deciphering operation.

Incremental deciphering refers to an operation and/or process used in block encryption/decryption as opposed to stream encryption/decryption. It is to be understood that incremental deciphering is the deciphering operation that takes place in a particular round of deciphering. With respect to incremental deciphering in different rounds, claim 1 calls for "*incrementally deciphering a ciphered text for a first round ... incrementally deciphering the partially deciphered text for a second round*". The deciphering is incremental because a round key partially deciphers the ciphered text block as opposed to completely deciphering that text block. With respect to partially deciphered text, claim 1 also calls for "*incrementally deciphering a ciphered text for a first round ... to generate a partially deciphered text*". Application of a multiplicity of round keys, each in its own particular round of deciphering, to the same text block in its successively partially deciphered state can ultimately produce the completely deciphered text block. With respect to the different round keys used, claim 1 calls for "*generating in real time a first deciphering round key based on a deciphering key ... generating in real time a second deciphering round key based, at least in part, on said generated first deciphering round key while said incremental deciphering for a said first round is being performed.*"

Incremental deciphering is not taught by Wright, separately or in combination with the other references. Wright clearly uses only one stream cipher to completely decipher or encipher a particular packet. *See Wright, col. 8, lines 8-16.* The packet is completely deciphered by a single application of only one stream cipher produced by the secondary key. After application of the stream cipher, the packet is clear text and is no longer in need of any further deciphering. This is in contrast to the method in claim 1

where application of a round key accomplishes incremental deciphering and produces a partially deciphered text, not completely deciphered after a first round. If Wright's application of the stream cipher were even remotely considered to be a round, and Assignee's representative does not agree with that characterization, it would be clear that deciphering in Wright would be completely accomplished after one round without a need for further rounds to further decipher the partially deciphered text associated with that one packet. As a result, Wright fails to teach, show, or suggest incremental deciphering as claimed in the present application.

Nakamura has been added to the combination apparently to provide a sense of real-time operation. But Nakamura appears to teach real-time operation for the encryption operation only. Encryption and decryption are completely different operations. Nakamura evidences no concern for real-time decryption operation, in general, or real-time round key generation for decryption, in particular. Nakamura is completely silent about the manner in which keys are generated for decryption. As a result, the addition of Nakamura to Wright and Coppersmith fails to teach, show, or suggest *"generating in **real time** a first deciphering round key based on a deciphering key"* and *"generating in **real time** a second deciphering round key based, at least in part, on said generated first deciphering round key while said incremental deciphering for a said first round is being performed"*, as claimed in the present application.

Coppersmith has been added to the combination apparently to provide a sense of rounds. Coppersmith appears to involve block encryption/decryption and the use of round keys, called sub-keys, in different rounds to encrypt/decrypt text. Coppersmith even appears to describe the prior generation and, if desired, the storage of the round keys. But Coppersmith does this for encryption only. *See Coppersmith, Figs. 5a & 5b and col. 20, lines 60-67.* Coppersmith is completely silent about the generation process for the decryption sub-keys (round keys) and, as a result of that silence, Coppersmith is completely silent about the time at which particular sub-keys are generated for decryption. Coppersmith teaches nothing about, for example, *"generating in real time a second deciphering round key based, at least in part, on said generated first deciphering round key while said incremental deciphering for a said first round is being performed"*, as claimed in the present application. Thus, even though Coppersmith appears to teach

the use of rounds, the addition of Coppersmith to the combined teachings of Wright and Nakamura cannot cure the deficiencies of those teachings.

As a result, the combination of Wright, Nakamura, and Coppersmith fail to teach, show, or suggest all the elements of claim 1. Since this combination of references does not teach all the elements of claim 1, it is submitted that claim 1 would not have been obvious to a person of ordinary skill in the art upon a reading of this combination of references. Therefore, it is believed that claim 1 is allowable under 35 U.S.C. §103.

Claims 2-3 depend from claim 1, either directly or indirectly, and include all the limitations thereof. In view of the remarks above for base claim 1, it is submitted that claims 2-3 are allowable under 35 U.S.C. §103.

Claims 10 and 21 and the claims dependent therefrom, contain limitations similar to those discussed above with respect to claim 1. Therefore, in view of the remarks above, it is submitted that claims 10-12, 20-23, and 31 are allowable under 35 U.S.C. §103.

CONCLUSION

In view of the foregoing, it is respectfully submitted that all the claims pending in this patent application are in condition for allowance. Reconsideration and allowance of all the claims are respectfully solicited.

If, however, the Examiner believes that there are any unresolved issues requiring adverse final action in any of the claims now pending in the application, it is requested that the Examiner telephone Gregory C. Ranieri, Esq. at (503) 439-6500 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

In the event there are any errors with respect to the fees for this response or any other papers related to this response, the Director is hereby given permission to charge any shortages and credit any overcharges of any fees required for this submission to Deposit Account number 50-3703.

Respectfully submitted,

Dated: **January 29, 2007**

/Gregory C. Ranieri, Reg. No. 29,695/
Gregory C. Ranieri, Attorney of Record
Registration No. 29,695

BERKELEY LAW & TECHNOLOGY GROUP, LLP
1700 NW 167th Place, Suite 240
Beaverton, OR 97006
Phone: 503.439.6500
Customer Number: 43831